CLAIMS

What is claimed is:

1	1.	A method for applying a service to an encrypted packet comprising:
2		examining an encrypted packet;
3	•	determining whether an identifier associated with the service is present in the
4		encrypted packet;
5		if it is determined that the identifier is present in the encrypted packet, applying the
6		service to the encrypted packet.

- 1 2. The method of claim 1, further comprising the steps of:
- encrypting the packet, wherein said step of encryption includes establishing said identifier in the packet.
- 1 3. The method of claim 1, wherein said identifier is based on at least on an Internet Key 2 Exchange (IKE) ID stored in the packet.
- 1 4. The method of claim 3, wherein the Internet Key Exchange (IKE) ID comprises one
- 2 or more of ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV4_ADDR_SUBNET,
- 3 ID_IPV6_ADDR, ID_IPV6_ADDR_SUBNET, ID_IPV4_ADDR_RANGE,
- 4 ID_IPV6_ADDR_RANGE, ID_DER_ASN1_DN, ID_DER_ASN1_GN, and ID_KEY_ID.
- 1 5. The method of claim 1, wherein the identifier is based on at least an entry in a security association database.
- 1 6. The method of claim 1, wherein said identifier maps to quality of service (QoS)
- 2 group.
- The method of claim 2, wherein the identifier is established in a profile of the packet.

The method of claim 7, wherein the profile is an ISAKMP profile. 1 8. The method of claim 2, further comprising a step of pre-classification of the packet 1 9. prior to the step of encryption. 2 The method of claim 9, wherein the service that is applied is selected based on both 1 10. 2 the identifier and pre-classification. A method for applying a service to a packet comprising: 1 11. 2 encrypting the packet to create an encrypted packet; examining an identifier in the encrypted packet, wherein the identifier is based on an 3 IKE ID of the encrypted packet; 4 determining whether the identifier in the encrypted packet is associated with a service 5 to be applied to the encrypted packet; and 6 if it is determined that the identifier is associated with a service to be applied to the 7 encrypted packet, applying the service to the encrypted packet. 8 1 12. The method of claim 11, further comprising the step of: prior to the step of encrypting, pre-classifying the packet based on the contents of the 2 3 packet; wherein the service that is applied to the packet is selected partially based the step of 4 pre-classification and partially based on the identifier. 5 The method of claim 11, further comprising the step of: 1 13. during encryption, copying at least one bit into a header to identify a characteristic of 2

of the at least one bit and partially based on the identifier.

wherein the service that is applied to the packet is selected partially based on a value

3

4

5

the packet;

- 1 14. A computer-readable medium comprising one or more sequences of instructions,
- 2 which when executed by one or more processors, cause the one or more processors to carry
- 3 out the steps recited in claim 1.
- 1 15. A computer-readable medium comprising one or more sequences of instructions,
- 2 which when executed by one or more processors, cause the one or more processors to carry
- 3 out the steps recited in claim 2.
- 1 16. A computer-readable medium comprising one or more sequences of instructions,
- 2 which when executed by one or more processors, cause the one or more processors to carry
- 3 out the steps recited in claim 3.
- 1 17. A computer-readable medium comprising one or more sequences of instructions,
- 2 which when executed by one or more processors, cause the one or more processors to carry
- 3 out the steps recited in claim 4.
- 1 18. A computer-readable medium comprising one or more sequences of instructions,
- 2 which when executed by one or more processors, cause the one or more processors to carry
- 3 out the steps recited in claim 5.
- 1 19. A computer-readable medium comprising one or more sequences of instructions,
- 2 which when executed by one or more processors, cause the one or more processors to carry
- 3 out the steps recited in claim 6.
- 1 20. A computer-readable medium comprising one or more sequences of instructions,
- 2 which when executed by one or more processors, cause the one or more processors to carry
- 3 out the steps recited in claim 7.

- 1 21. A computer-readable medium comprising one or more sequences of instructions,
- 2 which when executed by one or more processors, cause the one or more processors to carry
- 3 out the steps recited in claim 8.
- 1 22. A computer-readable medium comprising one or more sequences of instructions,
- which when executed by one or more processors, cause the one or more processors to carry
- 3 out the steps recited in claim 9.
- 1 23. A computer-readable medium comprising one or more sequences of instructions,
- 2 which when executed by one or more processors, cause the one or more processors to carry
- 3 out the steps recited in claim 10.
- 1 24. A computer-readable medium comprising one or more sequences of instructions,
- 2 which when executed by one or more processors, cause the one or more processors to carry
- 3 out the steps recited in claim 11.
- 1 25. A computer-readable medium comprising one or more sequences of instructions,
- 2 which when executed by one or more processors, cause the one or more processors to carry
- 3 out the steps recited in claim 12.
- 1 26. A computer-readable medium comprising one or more sequences of instructions,
- 2 which when executed by one or more processors, cause the one or more processors to carry
- 3 out the steps recited in claim 13.
- 1 27. An apparatus for applying a service to an encrypted packet comprising:
- 2 means for examining an encrypted packet;
- means for determining whether an identifier associated with the service is present in
- 4 the encrypted packet;

- 5 means for applying the service to the encrypted packet if it is determined that the
- 6 identifier is present in the encrypted packet.
- 1 28. The apparatus of claim 27, further comprising means for encrypting the packet,
- 2 wherein the means for encryption includes means for establishing said identifier in the
- 3 packet.
- 1 29. The apparatus of claim 27, wherein said identifier is based on at least on an Internet
- 2 Key Exchange (IKE) ID stored in the packet.
- 1 30. The apparatus of claim 29, wherein the Internet Key Exchange (IKE) ID comprises
- one or more of ID IPV4 ADDR, ID FQDN, ID USER FQDN,
- 3 ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR, ID_IPV6_ADDR_SUBNET,
- 4 ID IPV4 ADDR RANGE, ID IPV6 ADDR RANGE, ID DER ASN1 DN,
- 5 ID_DER_ASN1_GN, and ID_KEY_ID.
- 1 31. The apparatus of claim 27, wherein the identifier is based on at least an entry in a
- 2 security association database.
- 1 32. The apparatus of claim 27, wherein said identifier maps to quality of service (QoS)
- 2 group.
- 1 33. The method of claim 2, wherein the identifier is established in a profile of the packet.
- 1 34. The method of claim 7, wherein the profile is an ISAKMP profile.
- 1 35. The method of claim 2, further comprising means for pre-classification of the packet
- 2 prior to the step of encryption.

- 1 36. The method of claim 9, wherein the service that is applied is selected based on both
- 2 the identifier and pre-classification.
- 1 37. An apparatus for applying a service to an encrypted packet comprising:
- 2 one or more processors;
- memory communicatively coupled to the one or more processors;
- 4 one or more sequences of instructions in the memory for applying a service to an
- 5 encrypted packet, which instructions, when executed by the one or more
- 6 processors, cause the one or more processors to perform the steps of:
- 7 examining an encrypted packet;
- 8 determining whether an identifier associated with the service is present in the
- 9 encrypted packet;
- if it is determined that the identifier is present in the encrypted packet, applying the
- service to the encrypted packet.
- 1 38. The apparatus of claim 37, further comprising sequences of instructions for
- 2 performing the steps of:
- 3 encrypting the packet, wherein said step of encryption includes establishing said
- 4 identifier in the packet.
- 1 39. The apparatus of claim 37, wherein said identifier is based on at least on an Internet
- 2 Key Exchange (IKE) ID stored in the packet.
- 1 40. The apparatus of claim 39, wherein the Internet Key Exchange (IKE) ID comprises
- 2 one or more of ID IPV4 ADDR, ID FQDN, ID USER FQDN,
- 3 ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR, ID_IPV6_ADDR_SUBNET,
- 4 ID IPV4 ADDR RANGE, ID IPV6 ADDR RANGE, ID DER ASN1 DN,
- 5 ID DER ASN1 GN, and ID KEY ID.

- 1 41. The apparatus of claim 37, wherein the identifier is based on at least an entry in a
- 2 security association database.
- 1 42. The apparatus of claim 37, wherein said identifier maps to quality of service (QoS)
- 2 group.
- 1 43. The apparatus of claim 38, wherein the identifier is established in a profile of the
- 2 packet.
- 1 44. The apparatus of claim 43, wherein the profile is an ISAKMP profile.
- 1 45. The apparatus of claim 38, further comprising a step of pre-classification of the
- 2 packet prior to the step of encryption.
- 1 46. The apparatus of claim 45, wherein the service that is applied is selected based on
- 2 both the identifier and pre-classification.